

# ABSTRACT OF THE DISCLOSURE

The present invention provides permutation instructions which can be used in software executed in a programmable processor for solving permutation problems in cryptography, multimedia and other applications. The permute instructions are based on a Benes network comprising two butterfly networks of the same size connected back-to-back. Intermediate sequences of bits are defined that an initial sequence of bits from a source register are transformed into. Each intermediate sequence of bits is used as input to a subsequent permutation instruction. Permutation instructions are determined for permitting the initial source sequence of bits into one or more intermediate sequence of bits until a desired sequence is obtained. The intermediate sequences of bits are determined by configuration bits. The permutation instructions form a permutation instruction sequence of at least one instruction. At most  $2lgr/m$  permutation instructions are used in the permutation instruction sequence, where  $r$  is the number of  $k$ -bit subwords to be permuted, and  $m$  is the number of network stages executed in one instruction. The permutation instructions can be used to permute  $k$ -bit subwords packed into an  $n$ -bit word, where  $k$  can be 1, 2, ..., or  $n$  bits, and  $k*r=n$ .